07021 Abstracts Collection
Symmetric Cryptography
— Dagstuhl Seminar —

Eli Biham[1], Helena Handschuh[2], Stefan Lucks[3] and Vincent Rijmen[4]

[1] Technion - Haifa, IL
biham@cs.technion.ac.il
[2] Spansion, Levallois-Perret, FR
helena.handschuh@spansion.com
[3] Univ. Mannheim, DE
lucks@th.informatik.uni-mannheim.de
[4] TU Graz, AT
Vincent.Rijmen@iaik.tugraz.at

Abstract. From .. to .., the Dagstuhl Seminar 07021 "Symmetric Cryptography" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Authenticity, Integrity, Privacy, Block Ciphers, Stream Ciphers, Hash Functions, Provable Security, Cryptanalysis

07021 Executive Summary – Symmetric Cryptography

The Seminar brought together about 35 researchers from industry and academia. Most of the participants came from different European countries, but quite a few also came from America and Asia. Almost all the participants gave a presentation. Most of them gave a "regular" talk of 30 to 50 minutes (including discussion time), some gave a "rump session" talk, and a few even gave two presentations, a regular one and another at the rump session.

Keywords: Authenticity, Integrity, Privacy, Block Ciphers, Stream Ciphers, Hash Functions, Provable Security, Cryptanalysis

Joint work of: Biham, Eli; Handschuh, Helena; Lucks, Stefan; Rijmen, Vincent

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2007/1020

Seven-Property-Preserving Iterated Hashing: The RMC Construction

Elena Andreeva (Katholieke Universiteit Leuven, B)

Nearly all modern hash functions are constructed by iterating a compression function.

These compression functions are assumed to be secure relative to some security notion, like collision resistance, and we say the notion is preserved by the construction if the iterated hash is also secure relative to the notion. At FSEŠ04, Rogaway and Shrimpton [RS04] formalized seven security notions for hash functions: collision resistance (Coll), three variants of second-preimage resistance (Sec, aSec, eSec), and three variants of preimage resistance (Pre, aPre, ePre). In this paper determine, by proof or counterexample, which of these seven notions is preserved by existing iterated constructions. It turns out that none of strengthened Merkle-Damgard, Prefix-free Merkle- Damgard, Enveloped Merkle-Damgard Linear Hash, XOR-Linear Hash, Shoup's Hash, Randomized Hash, or HAIFA preserves all seven notions. In particular, all fail to preserve (at least) aSec and aPre. We propose a new iterated hash function, the Randomized Mask-then- Compress (RMC) construction, and prove that it is the first to preserve all of the notions. It does this using a salt, and a small random oracle that is called only a logarithmic number of times in the number of message blocks.

Keywords: Cryptographic hash functions, Merkle-Damgard hash, collision resistance, preimage resistance, second-preimage resistance, provable security

See also: [RS04] Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In Bimal K. Roy and Willi Meier, editors, Fast Software Encryption 2004, volume 3017 of Lecture Notes in Computer Science, pages 371-388. Springer- Verlag, Berlin, Germany, 2004.

Concealed data aggregation in wireless sensor networks

Frederik Armknecht (NEC Europe - Heidelberg, D)

Reducing the total required energy in a wireless sensor network is an outstanding goal. As sending one bit requires the same amount of energy as executing 50 to 150 instructions on sensor nodes, reducing the network traffic as much as possible is a substantial task. A widely discussed approach is the in-network aggregation of the sensed data.

Another serious issue is the security of the data. Considered that the data is transmitted encrypted, there is the problem of making aggregation possible without giving to much knowledge to the usually non-tamper resistant nodes. An

approach that promises the combination of end-to-end security and in-network aggregation is the concealed data aggregation (CDA).

The talk gives an overview on the topic of CDA, discusses some existing solutions, and points out open problems.

Block Ciphers and Stream Ciphers and the Creatures in Between

Alex Biryukov (University of Luxembourg, L)

In this paper we define a notion of leak extraction from a block cipher. We demonstrate this new concept on an example of AES. A result is LEX: a simple AES-based stream cipher which is at least 2.5 times faster than AES both in software and in hardware.

Keywords: Stream ciphers, block ciphers

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2007/1038

Algebraic Attacks On Block Ciphers

Nicolas T. Courtois (University College London, GB)

In this talk I will present some recent results concerning algebraic attacks on block ciphers.

Keywords: Algebraic cryptanalysis, block ciphers, DES, AES

How Fast ca be Algebraic Attacks on Block Ciphers?

Nicolas T. Courtois (University College London, GB)

In my talk I did overwiev the area of algebraic attacks on block ciphers, explain what fast algebraic attacks on block cipher are, and what results can already be achieved. This covers a vast amount of work (several papers, most of them not published) that I cannot include here in totality due to the lack of space.

Keywords: Algebraic Attacks On Block Ciphers, XSL attacks, AES, DES, SAT Solvers, T' method, Gröbner bases

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/1013

Sponge functions

Joan Daemen (STMicroelectronics - Zaventem, B)

Ideally, cryptographic hash function should not be easier to attack than random oracles. Most practical cryptographic hash functions are iterated and exhibit internal collisions.

These internal collisions are a weakness that random oracles do not have and can be used in several attack scenario's. Examples are multicollision attacks [Joux], 2nd-preimage attacks [Kelsey Schneier] and herding attacks [Kelsey, Kohno].

We propose an alternative for the random oracle in this context: a random sponge. A sponge is a simple construction that implements a variable-length input, infinite length output function making use of a permutation. In some sense, a random sponge is the closest to a random oracle with an iterated function operating on a finite state: we prove that in the absence of inner collisions the output has exactly the same distribution as a random oracle. On the other hand, by increasing the capacity, a parameter that models the size of the internal state, the generation of internal collisions can be made arbitrarily difficult.

Random sponges may serve as reference for what a concrete hash function should satisfy: designers may specify that their hash function is considered to be broken when there is an attack that is more successful than for a random sponge with given capacity. The sponge structure also give inspiration for design leading to cleaner constructions.

Keywords: Cryptographic hash functions

Joint work of: Daemen, Joan; Bertoni Guido, Peeters Michaël; Van Assche, Gilles

Finding SHA-1 Characteristics

Christophe De Cannière (Katholieke Universiteit Leuven, B)

In this talk, we will present techniques for constructing SHA-1 characteristics. We will discuss how these characteristics look like in general, develop metrics to evaluate them, and propose strategies to search for characteristics optimizing these metrics.

Joint work of: De Canniere, Christophe; Rechberger, Christian

Keyless Postprocessing of Pseudorandom Bit Sequences, a Good Means to Increase their Cryptographic Strength?

Markus Dichtl (Siemens - München, D)

I will look at several known methods of keyless postprocessing for pseudorandom bit sequences. Some turn out to work well, some not. I will also suggest a new method and will discuss some of its properties.

Keywords: Streamcipher, pseudorandom, postprocessing

Cryptographic Shuffling of Random and Pseudorandom Sequences

Markus Dichtl (Siemens - München, D)

This papers studies methods to improve the cryptographic quality of random or pseudorandom sequences by modifying the order of the original sequence. A new algorithm Cryshu is suggested, which produces its shuffled output data at the rate of the input data.

Keywords: Shuffling stream-cipher

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/1014

A Unified Approach to Related-Key Attacks

Orr Dunkelman (Katholieke Universiteit Leuven, B)

In this talk we introduce a new framework and a generalization of the various flavors of related-key attacks. The new framework allows for combining all the previous related-key attacks into a complex, but much more powerful attack. The new attack is independent of the number of rounds of the cipher. This property holds even when the round functions of the cipher use different subkeys.

The new attack can be applied to a wide variety of ciphers, including ciphers that were previously considered immune to related-key attacks.

The strength of our new method is demonstrated by an attack on $4r$-round IDEA, for any r. This attack is the first attack on a widely deployed block cipher which is independent of the number of rounds.

The variant of the attack with $r = 2$ is the first known attack on 8-round IDEA.

Keywords: Related-Key Attacks, IDEA, Slide Attack

Joint work of: Dunkelman, Orr; Biham, Eli; Keller, Nathan

QUAD: overview and recent developments

Henri Gilbert (France Telecom - Issy Les Moulineaux, F)

In this talk I will first give an outline of the main features of the QUAD stream cipher initially proposed at Eurocrypt '06, and an overview of the reduction of the security of the keystream generation to the intractability of solving a random system of $2n$ equations in n unknowns over GF(2).

I will also describe some more recent developments related to QUAD:

- Hardware and software performance: it will be shown that if one is willing to pseudorandomly generate the systems of quadratic polynomials underlying

QUAD, then this leads to a suprisingly inexpensive hardware implementation (only 3500 g.e. for some parameter choices).

- Finally, an extension of the initial security argument to incorporate the IV loading.

Keywords: Stream ciphers, quadratic equations, provable security, multivariate cryptography

Joint work of: Gilbert, Henri; Arditti, David, Berbain, Côme; Billet, Olivier; Patarin, Jacques

QUAD: Overview and Recent Developments

Henri Gilbert (France Telecom - Issy Les Moulineaux, F)

We give an outline of the specification and provable security features of the QUAD stream cipher proposed at Eurocrypt 2006.

The cipher relies on the iteration of a multivariate system of quadratic equations over a finite field, typically GF(2) or a small extension. In the binary case, the security of the keystream generation can be related, in the concrete security model, to the conjectured intractability of the MQ problem of solving a random system of m equations in n unknowns. We show that this security reduction can be extended to incorporate the key and IV setup and provide a security argument related to the whole stream cipher.We also briefly address software and hardware performance issues and show that if one is willing to pseudorandomly generate the systems of quadratic polynomials underlying the cipher, this leads to suprisingly inexpensive hardware implementations of QUAD.

Keywords: MQ problem, stream cipher, provable security, Gröbner basis

Joint work of: Arditti, David; Berbain, Côme; Billet, Olivier; Gilbert, Henri; Patarin, Jacques

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/1015

Block ciphers to encrypt unusual domains

Louis Granboulan (EADS-Suresnes, F)

While usual block ciphers are pseudo-random permutations of the set of 64-bit or 128-bit strings, it might be useful to have block ciphers that permute arbitrary sets. Here we consider designs of such block ciphers, and we avoid using usual block ciphers as building blocks. We describe directions for three types of unusual domains: blocks being numbers in base $p \neq 2$; sets of small size, typically $2^3 2$; set of points of an elliptic curve.

Keywords: Block cipher

Blind Differential Cryptanalysis for Enhanced Power Attacks

Helena Handschuh (Spansion - Levallois-Perret, F)

At FSE 2003 and 2004, Akkar and Goubin presented several masking methods to protect iterated block ciphers such as DES against Differential Power Analysis and higher-order variations thereof. The underlying idea is to randomize the first few and last few rounds of the cipher with independent masks at each round until all intermediate values depend on a large number of secret key bits, thereby disabling power attacks on subsequent inner rounds. We show how to combine differential cryptanalysis applied to the first few rounds of the cipher with power attacks to extract the secret key from intermediate unmasked (unknown) values, even when these already depend on all secret key bits. We thus invalidate the widely believed claim that it is sufficient to protect the outer rounds of an iterated block cipher against side-channel attacks.

Keywords: Differential cryptanalysis, power analysis, side channel attacks

Joint work of: Handschuh, Helena; Preneel, Bart

See also: To appear in the proceedings of Selected Areas in Cryptography, Montreal, August 2006

Tightness of the Security Bound of CENC

Tetsu Iwata (Nagoya University, J)

This talk presents an overview of recently developed encryption mode for blockciphers, called CENC.

CENC has the following advantages:

1. beyond the birthday bound security,
2. security proofs with the standard PRP assumption,
3. highly efficient,
4. single blockcipher key,
5. fully parallelizable,
6. allows precomputation of keystream, and
7. allows random access.

Then we discuss the tightness of its security bound, and give a partial answer to the open problem posed at FSE 2006.

Keywords: Encryption mode, blockcipher, CENC, provable security

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/1016

Full Paper:
http://www.nuee.nagoya-u.ac.jp/labs/tiwata/

On the computation of differential characteristics for arbitrary S-Boxes

Antoine Joux (University of Versailles, F)

In this talk, we revisit the Walsh transform and its well-known application to the computation of linear characteristics. We show that it can also be used to compute differential characteristics. After that, we present a generalization that very efficiently address the problem of computing truncated differential characteristics.

On Boolean Functions with Maximal Algebraic Immunity

Matthias Krause (Universität Mannheim, D)

We construct boolean functions f from $\{0,1\}^n$ to $\{0,1\}^m$ for which the graph $gr(f) = \{(x, f(x)); x \in \{0,1\}^n\}$ has maximal algebraic immunity. This research is motivated by making building blocks of symmetric cryptosystems immune against algebraic attacks. we completely solve the problem of constructing single-output boolean functions for which the graph has maximal algebraic immunity. Concerning multi-output functions we present an efficient algorithm, based on matroid union, which computes for given n, m, d the table of function with n input and m output bits for which the immunity of the graph is at least d. To the best of our knowledge, this is the first systematic method for constructing multioutput functions of high immunity.

Keywords: Algebraic immunity, boolean functions

Joint work of: Krause, Matthias; Armknecht, Frederik

On Block Cipher Based Hash Functions

Stefan Lucks (Universität Mannheim, D)

This talk presents a new construction for 2n-bit hash functions, based on an n-bit block cipher with 2n-bit keys. The hash function runs at rate one and is proven collision-resistant in the ideal cipher model. Further, this talk discusses block cipher based hash functions in general, and the usage of the ideal cipher model for proving hash function security.

A Collision-Resistant Rate-1 Double-Block-Length Hash Function

Stefan Lucks (Universität Mannheim, D)

This paper proposes a construction for collision resistant $2n$-bit hash functions, based on n-bit block ciphers with $2n$-bit keys.

The construction is analysed in the ideal cipher model; for $n = 128$ an adversary would need roughly 2^{122} units of time to find a collision.

The construction employs "combinatorial" hashing as an underlying building block (like Universal Hashing for cryptographic message authentication by Wegman and Carter).

The construction runs at rate 1, thus improving on a similar rate 1/2 approach by Hirose (FSE 2006).

Keywords: Hash function, provable security, double-block-length

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/1017

Algebraic Immunity of S-boxes and Augmented Functions

Willi Meier (FH Nordwestschweiz - Brugg, CH)

The algebraic immunity of S-boxes and augmented functions of stream ciphers is investigated. Augmented functions are shown to have some algebraic properties that are not covered by previous measures of immunity. As a result, efficient algebraic attacks with very low data complexity on certain filter generators become possible. This has been experimentally tested. Our investigation allows to contribute to open problems in the context of algebraic attacks using Gröbner bases against filter generators: Why in certain cases such attacks are successful even for a very short known output segment.

In a similar line, the algebraic immunity of the augmented function of the eSTREAM candidate Trivium is experimentally tested. These tests suggest that Trivium has some immunity against algebraic attacks on augmented functions. Such experiments become feasible as for Trivium with its 288-bit state one can find preimages of 144-bit outputs in polynomial time.

Augmented functions of LFSR-based stream ciphers have previously been studied. It had been noticed that the augmented function can be weaker than a single output function, with regard to (conditional) correlation attacks as well as to inversion attacks. However, for the first time, we analyse the algebraic immunity of (sometimes quite large!) augmented functions. Surprisingly, augmented functions did not receive much attention in this context yet.

Joint work of: Meier, Willi; Fischer, Simon

Update on Tiger

Florian Mendel (TU Graz, A)

Tiger is a cryptographic hash function with a 192-bit hash value which was proposed by Anderson and Biham in 1996. At FSE 2006, Kelsey and Lucks presented a collision attack on Tiger reduced to 16 (out of 24) rounds with complexity of about 2^{44}.

Furthermore, they showed that a pseudo-near-collision can be found for a variant of Tiger with 20 rounds with complexity of about 2^{48}.

In this article, we show how their attack method can be extended to construct a collision in the Tiger hash function reduced to 19 rounds. We present two different attack strategies for constructing collisions in Tiger-19 with complexity of about 2^{62} and 2^{69}. Furthermore, we present a pseudo-near-collision for a variant of Tiger with 22 rounds with complexity of about 2^{44}.

Keywords: Cryptanalysis, hash functions, differential attack, collision, near-collision, pseudo-collision, pseudo-near-collision

Joint work of: Mendel, Florian; Rijmen, Vincent; Preneel, Bart; Yoshida, Hirotaka; Watanabe, Dai

See also: Florian Mendel, Bart Preneel, Vincent Rijmen, Hirotaka Yoshida, and Dai Watanabe, Update on Tiger. In Proceedings of Progress in Cryptology - INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11-13, 2006, pp. 63-79, LNCS 4329.

Technical Aspects of PLAYSTATION 3

Shiho Moriai (Sony - Tokyo, J)

This talk will give technical aspects of PLAYSTATION 3, which was launched in November 2006 in Japan and US. It is currently scheduled it is launched in March 2007 in Europe. The talk includes the Cell Broadband Engine, Blu-ray Disc, network connectivity, SIXAXIS wireless controller, high-definition capabilities, HDD, system interoperability and backwards compatibility.

A Key-Recovery Attack on SOBER-128

Kaisa Nyberg (Helsinki University of Technology, FIN)

In this talk we consider linear approximations of layered cipher constructions with secret key-dependent constants that are inserted between layers, and where the layers have strong interdependency. Then clearly, averaging over the constant would clearly be wrong as it will break the interdependencies, and the Piling Up -lemma cannot be used. We show how to use linear approximations to divide the constants into constant classes, not necessary determined by a linear relation. As an example, a nonlinear filter generator SOBER-128 is considered and we show how to extend Matsui's Algorithm I in this case. Also the possibility of using multiple linear approximations simultaneously is considered.

Keywords: Linear approximations, correlation, linear cryptanalysis, key recovery attack, piling-up lemma, SOBER-128

Joint work of: Nyberg, Kaisa; Risto, Hakala

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/1018

Structural Analysis of SMASH

Norbert Pramstaller (TU Graz, A)

At FSE 2005, Knudsen proposed a new hash function design strategy called SMASH. In this talk we present a detailed structural analysis of the design strategy. First, we show how one can construct collisions for SMASH by exploiting structural properties of the hash function. Secondly, we generalize the collision attack resulting in second preimages for SMASH.

Joint work of: Lamberger, Mario; Pramstaller, Norbert; Rechberger, Christian; Rijmen, Vincent

Cryptanalysis of eSTREAM Phase 2 ciphers

Bart Preneel (Katholieke Universiteit Leuven, B)

We present efficient key recovery attacks on several eSTREAM Phase 2 stream ciphers. These include ABC (v2 and v3), Py (also PyPy and P6) and Phelix. Our attacks use weak keys and differential cryptanalysis with related or chosen IVs. They have in common that they require less than 2^{40} words of key stream and that they recover (part of) the key with a complexity of less than 2^{40}.

Keywords: Stream ciphers, differential cryptanalysis, weak keys, related IV

Joint work of: Preneel, Bart; Wu, Hongjun

Finding Generalized Characteristics: Applications and Open Problems

Christian Rechberger (TU Graz, A)

As a follow-up of the talk "Finding SHA-1 Characteristics", we will discuss applications of generalized characteristics, and open problems in this context.

Joint work of: De Canniere, Christophe; Rechberger, Christian

Plateau characteristics

Vincent Rijmen (TU Graz, A)

Plateau characteristics are a special type of characteristics whose probability depends on the key and can have only 2 values.

For a (usually small) subset of the keys it has a non-zero probability and for all other keys its probability is zero. We show that for a large group of ciphers, including the AES, all two-round characteristics are plateau characteristics. For the AES and other ciphers with a similar structure, the vast majority of characteristics over 4 or more rounds are plateau characteristics. In the case of the AES, for most keys there are two-round characteristics with fixed-key probability equal to $32/2^{-32}$ while the Maximum Expected Differential Probability (MEDP) of two-round differentials is at most $13.25/2^{-32}$.

Keywords: Differential cryptanalysis, AES

Joint work of: Rijmen, Vincent; Daemen, Joan

Formalizing Human Ignorance: Collision-Resistant Hashing without the Keys

Phillip Rogaway (Univ. of California - Davis, USA)

There is a rarely mentioned foundational problem involving collision-resistant hash-functions: common constructions are keyless, but formal definitions are keyed. The discrepancy stems from the fact that a function $H : 0,1^* -> 0,1^n$ always admits an efficient collision-finding algorithm, it's just that us human beings might be unable to write the program down.

We explain a simple way to sidestep this difficulty that avoids having to key our hash functions. The idea is to state theorems in a way that prescribes an explicitly-given reduction, normally a black-box one. We illustrate this approach using well-known examples involving digital signatures, pseudorandom functions, and the Merkle-Damgard construction.

Full Paper:
http://www.cs.ucdavis.edu/~rogaway/papers/ignorance.pdf

Design and Primitive Specification for Shannon

Gregory G. Rose (Qualcomm Inc. - San Diego, USA)

Shannon is a synchronous stream cipher with message authentication functionality, designed according to the ECrypt NoE call for stream cipher primitives, profile 1A (but well after the call).

Shannon is named in memory of Claude E. Shannon of Bell Labs and MIT, founder of Information Theory. Shannon is an entirely new design, influenced by members of the SOBER family of stream ciphers, Helix, Trivium, Scream, and SHA-256. It consists of a single 32-bit wide, 16 element nonlinear feedback shift register, which is supplemented for message authentication with 32 parallel CRC-16 registers.

Keywords: Stream cipher

Joint work of: Rose, Gregory G.; Hawkes, Philip; Paddon, Michael; McDonald, Cameron; Wiggers de Vries, Miriam

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/1019

BDD-Attacks on Stream Ciphers

Dirk Stegemann (Universität Mannheim, D)

Stream ciphers are primarily used for online-encryption of arbitrarily long data, for example when transmitting speech data between a Bluetooth headset and a mobile phone. Many practically used and intensively discussed stream ciphers consist of a small number of linear feedback shift registers (LFSRs) that transform a secret key $x \in \{0,1\}^n$ into an output keystream of arbitrary length. In 2002, Krause showed how to use Binary Decision Diagrams (BDDs) to mount a generic attack on this type of ciphers that recovers the secret key from the shortest information-theoretically possible amount of output keystream. In the case of the Bluetooth cipher E_0, this attack is the best currently known short-keystream attack. Unlike correlation attacks and algebraic attacks, the BDD-attack is also applicable to irregularly clocked stream ciphers like the GSM cipher A5/1. In this talk, we describe the BDD-attack and its application to A5/1 and E_0 in theory and practice, show how to reduce its memory consumption, and sketch some recent developments.

Keywords: Stream cipher, LFSR, E0, A5/1, BDD-attack

When Stream Cipher Analysis Meets Public-Key Cryptography

Serge Vaudenay (EPFL - Lausanne, CH)

We present a new public-key cryptosystem, a hardware-oriented public-key cryptosystem, whose security relies on the hardness of problem coming from stream cipher analysis: the problem of finding a low-weight multiple of a given polynomial. Our improvement makes it possible to decrypt in polynomial time (instead of exponential time) and to directly prove semantic security (instead of one-wayness). We further build IND-CCA secure schemes using the KEM/DEM and Fujisaki-Okamoto hybrid encryption frameworks in the random oracle model. This can encrypt an arbitrary message with an overhead of about 5 Kb in less than 15 ms, on an ASIC of about 10,000 gates at 4 MHz.

Keywords: Low-weight multiple, public-key cryptosystem, stream cipher analysis

Joint work of: Aumasson, Jean-Philippe; Finiasz, Matthieu; Meier, Willi; Vaudenay, Serge

How cryptography interacts with legal safeguards

Marion Videau (LORIA - Nancy, F)

The research topic that is presented here has no strong relations with symmetric cryptography and is more intended to consist in some kind of rump session talk.

It deals with what has always been a border of cryptography, that is to say law. The very aspect underlined here concerns electronic writing and the keeping of evidence. We take the example of the French law which had claimed the equivalence between handwritten signature and digital signature in 2001. We present some consequences of this choice regarding the problem of evidence creation and keeping as for contracts.

It highlights the fact that adapting to digital environment is not straightforward from law point of view, but also that cryptographic tools may not be adapted to law requirements at all.

Keywords: Cryptography, law, record management, digital signature

Recovering S-Boxes by solving polynomial equations

Ralph-Philipp Weinmann (TU Darmstadt, D)

For licensing reasons, DRM schemes may want to implement ciphers with secret S-Boxes. For example, the block cipher C2 of the CPRM scheme has a secret 8-bit S-Box.

In a chosen-text, chosen-key model, we investigate how this specific S-Box could be recovered using a combination of a differential attack and solving polynomial equations. From the carefully chosen plaintext/ciphertext pairs we obtain sufficient information to expect a unique solution for a large polynomial system over GF(2); yielding a number of entries of the secret S-Box.

Keywords: Block ciphers, secret s-boxes, polynomial systems, algebraic cryptanalysis

Joint work of: Weinmann, Ralph-Philipp; Kuehn, Ulrich

Data-at-Rest Encryption: Issues and Standards

Doug Whiting (Hifn - Carlsbad, USA)

This presentation outlines the current standards activities in IEEE P1619 dealing with encryption of data at the physical block level (not the file level) on disk and tape. There is no universal agreement (yet) on all the threat models to be addressed, and these standards are not intended for data interchange. Rather severe constraints are imposed on the cryptography here due to backward compatibility requirements.

This talk will discuss some of the best understood threats addressed by the proposed standards, as well as the open issues and concerns.

Keywords: Data-at-Rest Storage Encryption

Why IV Setup for Stream Ciphers is Difficult

Erik Zenner (Cryptico - Copenhagen, DK)

In recent years, a large number of stream ciphers have been broken due to problems with their IV setup. When taking an engineering approach to designing a good IV setup (as opposed to a trial-and-error approach), we have to start by asking what such an IV setup is supposed to achieve.

As it turns out, all questions related to this issue are essentially unanswered. In this talk, we give an overview over these open questions.

Keywords: Initialization vectors, IV setup, stream cipher

Why IV Setup for Stream Ciphers is Difficult

Erik Zenner (Cryptico - Copenhagen, DK)

In recent years, the initialization vector (IV) setup has proven to be the most vulnerable point when designing secure stream ciphers. In this paper, we take a look at possible reasons why this is the case, identifying numerous open research problems in cryptography.

Keywords: Stream cipher, IV setup

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/1012